Business Secure Router BSR252

Release Notes

Firmware Version 2.6.0.0.005b1

Document ID:	RN5S20BA
Version:	3.0
Date:	11 June 2007
Status:	Released
Authors:	Dave Denike

Table of Contents

Summary **1**

Problems Fixed in this Release 1

Enhancements Added in this Release 1

General User Notes **2**

Known Issues **5**

NOTICE

This document contains confidential information, which is proprietary to Nortel Inc.
No part of its contents may be used, copied, disclosed or conveyed to any party in any manner whatsoever without prior written permission from Nortel.

Summary

This document provides an overview of the firmware release 2.6.0.0.005b1 for the BSR252 Business Secure Router. This router supports Annex-A ADSL, ADSL2, and ADSL2+ connections.

Problems Fixed in this Release

The following problems were addressed since the last release (2.6.0.0.004):

Q01615395
Traffic outside of a split tunnel would not be sent if tunnel negotiation started, but failed.

Q01647312
The BSR252 would take a long time to get a new address, if a PC was disconnected from the BSR, connected to another gateway, and then connected back to the BSR in a short period.

Q01586160
The 'Apply' button in the Advanced VPN configuration was renamed, because it doesn't actually apply the changes that are made.

Q01641027
In the System»General GUI page, entries made in the System Name and Domain Name would disappear when the DNS Server pull-down menu was selected.

Enhancements Added in this Release

Q01586066
A warning message was added in the WAN»WAN ISP GUI page, if a PPPoE or PPPoA account is defined with a blank password.

General User Notes

There are some BSR252 functions that, although performing as expected, have been found by some users to cause some confusion. These are summarized below.

General

1. Default Address Mapping Rules When First Enable NAT Full Feature
   When NAT Full Feature is first enabled, two address mapping rules are added to the address mapping table. This is done to facilitate programming, and matches the default SUA rule. The rules can be deleted.

2. Response to Invalid User ID or Password
   When the wrong user ID or password is entered into the router login screen, no error message is displayed. Instead, the login screen is simply displayed again.

3. First DHCP Address Reserved for BCM50
   The first address of the DHCP Address Pool is reserved for a BCM50 in the subnet, and will not be assigned to any other equipment. Once assigned to a BCM50, it is reserved for that BCM50, and will not be assigned to any other. If the BCM50 is changed, the following command must be used to enable the router to assign the first address to a different BCM50:
   ```
   ip dhcp enif0 server m50mac clear
   ```

4. Login Requires Reboot
   If the Administrator Timeout is set to 0, and an administration session is terminated without logging off, the router needs to be rebooted in order for the administrator to log in to the WebGUI again. Alternatively, the administrator can log in using a TelNet session, if TelNet access has been enabled in the Remote Management menu.

Firewall

5. Address Range Validation
   In the firewall rules, the router does not confirm when given an address range, that the second address is higher than the first. If this type of address range is entered, the range is ignored.

6. Automatic Firewall Programming
   Configurations to various areas of the router, such as remote management or adding a SUA Server, do not automatically add the appropriate rules to the Firewall, to enable the traffic to pass through the router. These need to be added separately.

   Note: Firewall rules do not apply to IPSec tunnels.

NAT

7. Deleting NAT Rule Does Not Drop an Existing Connection
   If a NAT rule is deleted, the router must be rebooted to apply the change to existing service connections. This is already noted in the GUI.

8. Confusing NAT Traversal Status
   If NAT Traversal is enabled, but is not needed (because the client is not behind a NAT router), it will be shown as ‘inactive’ in the VPN Client Monitor. This may confuse some users.

Client and Branch Office Tunnels

9. Change of User Account Does Not Drop Existing Connections
   If a VPN Client user account is de-activated, deleted, or changed, and that user is currently

connected, the connection is not automatically dropped. To drop the connection, the administrator needs to disconnect the user using the 'Disconnect' function in the VPN/SA Monitor GUI. This is consistent with other Nortel Contivity products.

10. User Name Restrictions
    User names are limited to a maximum length of 63 characters.

11. VPN Client Account Password Restrictions
    The password for a VPN Client user cannot contain the single- or double-quote characters.

12. IP Pool Address Overlap
    When defining multiple VPN Client Termination IP pools, the router uses the IP Subnet mask, and not the pool size, to determine if the pools are overlapping. The subnet mask of each pool should be appropriate for the size of the VPN Client Termination IP pool.

13. VPN Client Termination - IP Address Restrictions
    If the Client has an assigned IP address that is the same as the IP address assigned for the Client Tunnel, the connection will fail to be established.

14. VPN Client Termination – Configuration Restrictions
    This router has some restrictions when compared to larger Contivity Routers (1000 Series and above). In particular,

    VPN Clients cannot be added to the LAN subnet. They must have addresses outside of the LAN subnet.

    VPN Clients can have dynamically assigned IP addresses, or they can have statically assigned addresses. However, the router does not support both modes at once. All addresses must either be dynamically assigned, or they must all be statically assigned.

15. BSR252 Client Emulation to BSR252 Client Termination Requires PFS to be Enabled
    To establish a client tunnel between two BSR252s or a BSR222 and a BSR252, Perfect Forward Secrecy needs to be enabled on the Client Termination side of the connection. This is found in the VPN Advanced Configuration, in the Phase 2 options.

Security

16. Exporting or Saving Self-Signed Certificate
    To export or save a self-signed certificate, click details (the icon that looks like a paper note), then click 'Export' or copy the PEM text into the clipboard, and paste into a file.

17. Enabling Firewall Drops Web Page Link
    When the firewall is enabled using the WebGUI, the WebGUI session is dropped, which seems as if the router has hung. The connection can be re-established by refreshing the web page.

Routing

18. RIP Version Advertisement Control
    To change the version of generated RIP advertisements, the following CLI command needs to be used
    `ip rip mode [enif0|enif1] [in|out] [0|1|2|3]`
    where:

    'enif0' is the LAN side, and 'enif1' is the WAN side

    'in' affects recognition of received advertisements, and
    'out' applies to generated advertisements

    The number controls the operating mode:

    0: None (disabled)

    1: RIP-1 only

    2: RIP-2 only

    3: Both RIP-1 and RIP-2

Bandwidth Management

19. Configuring Bandwidth Manager to Recognize SIP or H.323 Traffic
    To prioritize traffic from SIP telephones, a recommended approach is to choose an IP address range for the telephones within the LAN subnet, but outside of the DHCP pool, statically assign IP addresses to the telephones within that range, and prioritize all traffic from that address range.

20. Configuring the WAN Bandwidth
    In order for Bandwidth Management to work properly, the BSR252 needs to be configured with your actual upstream data rate that is provided by your Internet service. To determine this rate, connect to a Web site such as http://myvoipspeed.visualware.com/. Enter your upstream data rate in BSR252 GUI, in the WAN Speed field of the Bandwidth Management Summary page.

Known Issues

Known issues are summarized below, along with methods to work around them.

General

1. Q01664034 – Some Revisions of Contivity Client Cannot Be Rejected
   When the minimum version of Contivity Client is set to 6.1, connections with 5.1 clients are not rejected.
2. Q01664210 – Content Filter Access Denied Message Not Displayed with Internet Explorer 7
   An 'access denied' message is displayed when access is blocked by the Content Filter. With Internet Explorer version 7, this message is not displayed properly.

Client and Branch Office Tunnels

3. Q01664034 – Some Revisions of Contivity Client Cannot Be Rejected
   When the minimum version of Contivity Client is set to 6.1, connections with 5.1 clients are not rejected.
4. Q01650984 – Third VPN DHCP Pool Cannot Be Used
   Although three client address pools can be configured, the third pool cannot be selected.
5. Q01665250 – Establish Retries For Client Emulation ISAKMP Negotiation
   When a VPN server goes down and comes back up, it has to deal with a large number of simultaneous reconnect requests. To accommodate this, the router needs to retry ISAKMP negotiation, before giving up and starting over.
6. Q01664827 – Error Message is Wrong When Submitting a Conflicting VPN Tunnel IP Policy
   When a VPN Tunnel policy rule is submitted that conflicts with an existing policy rule, the resultant error message does not correctly identify the conflicting rule.

Bandwidth Management

7. Q01532949 – Configuring Bandwidth Manager to Recognize SIP or H.323 Traffic
   The Bandwidth Manager cannot recognize SIP or H.323 traffic unless the corresponding SIP or H.323 ALG is turned on. To prioritize traffic from SIP telephones, a recommended approach is to choose an IP address range for the telephones within the LAN subnet, but outside of the DHCP pool, statically assign IP addresses to the telephones within that range, and prioritize all traffic from that address range.

Routing

8. Q01617936 – If a device on the LAN side of the BSR252 is replaced with a different device that is statically assigned the same address as the original address, the original ARP table entry is not updated while traffic is actively being sent to that address.
9. Q01640156 – Fixed WAN Gateway Address and SUA
   If you are using a fixed Gateway IP address, and SUA Network Address Translation, then do the following on the WAN IP GUI page:

   Ensure the Gateway IP address is not set to 0.0.0.0, and Network Address Translation is set to 'None'. Save the setting.

   Set the Network Address Translation to 'SUA Only', and save the setting.